REMARKS

The above amendments and following remarks are submitted under 37 C.F.R. 1.116 in response to the Final Official Action of the Examiner mailed October 8, 2002. Having addressed all objections and grounds of rejection, claims 1-20, being all the pending claims, are now deemed in condition for allowance. Entry of these amendment and reconsideration to that end is respectfully requested.

The Examiner has objected to Fig. 10 of the drawings as not containing the reference number "331" contained at pages 33-34 of the amended specification. In response thereto, pages 33-34 of the specification has been amended above to removed the reference number "331".

The Examiner has objected to the specification alleging:

> The terms "User Validation Service" and "UserID/Password" are used in the specification to refer to different things. This fact renders relevant portions of the specification indefinite. (Emphasis added)

On its face, it would seem that the Examiner has objected to normal draftsmanship, wherein "User Validation Service" refers to something different from "UserID/Password". It is standard practice to utilize different terms to refer to different entities.

In further support of his objection, the Examiner, completely without authority, proceeds to redefine Applicants' terminology. He states:

> For instance, on page 7, lines 9-11, it is disclosed that the user signs in by entering a UserID and Password, which the examiner will refer to as the user-spcific UserID and Password. Later, at lines 12-14, it is disclosed that site-specific data is converted to a valid UserID and Password, which the examiner will refer to as site-specific UserID and Password. Further still, at lines 17-19, it is disclosed that 'information' is translated into a UserID and Password, which the examiner will refer to as the server UserID and Password. The use of these terms to refer to multiple instances adds confusion to the specification. (Emphasis as original)

Though not well understood, it appears that the Examiner has objected to the use of "UserID and Password" to refer to a digital quantity (a "UserID and Password" is expressible as a digital number) based upon how or where it is generated.

Certain models of Chevrolet automobiles are manufactured at Janesville, Wisconsin, and other models of Chevrolet automobiles are manufactured at Bowling Green, Kentucky. Yet, these diverse models, manufactured at different places may each be termed a Chevrolet automobile. Each has four wheels and an internal combustion engine; each requires a licensed driver; each requires a vehicle license; etc. Perhaps more important, the operation of each is similarly treated under the law with regard to traffic laws.

The Examiner has correctly noted that in the preferred mode of the present invention, "UserID's and Password's", though potentially indistinguishable in syntax and function in granting access to the claimed data base management system, may have been generated in a different manner or may refer to a specific individual and/or a specific site. That is Applicants' invention and that is why the Examiner has found Applicants' invention to be novel.

The Examiner makes an even more apparent mistake in logic with regard to the "User Validation Service". He states:

> The inconsistency is that on page 7, lines 19-20, it is disclosed that the invention precludes the need to send a UserID/Password from the browser to the server, but as stated above, the site-specific UserID/Password is indeed passed from the browser the server. Furthermore, on replacement page 34, lines 9-12, it is disclosed that the service handler requests the user to provide a UserID, and that UserID is transmitted via the Internet to the server, which is compared to the security profile of a requested script. Given these facts, there is inconsistency between the claimed feature of the invention (<u>that no UserID/Password is transmitted from the browser to server via the Internet</u>) and the disclosed details of the invention..... (emphasis added)

It is clear from the emphasized portion of this quotation, that the Examiner has not misread the specification but has misread Applicants' claims. The emphasized portion of the quotation above is clearly erroneous. Nowhere within the claims, do Applicants state that no "UserID/Password" need be transmitted over the network. However, in response to these objections, claims 1, 6, and 11 have been above amended to more clearly indicate that the personal "user identifier" of a specific user need not be transferred over the network. The claims do not preclude transfer of a site-specific "user identifier". On this basis, the objection to the specification is respectfully traversed.

The Examiner has rejected claims 1-20 under 35 U.S.C. 112, first paragraph. This ground of rejection is respectfully traversed. Having above found that Applicants disclose that a "user-specific UserID/Password" and a "site-specific UserID/Password" are indistinguishable in syntax and function and that the "site-specific UserID/Password" is transferred over the network, the Examiner confusingly states:

> ....the details of the use of the site specific security profile is not disclosed in the Detailed Description of the Preferred Embodiments, and in fact the section of the Detailed Description concerning the operation of security profiles discloses a mechanism whereby a user submits a service request which results in the execution of a command language script with associated security profile which require the user to submit a UserID over the World Wide Web in order for the execution of the script to proceed.

The Examiner has previously responded to his own rejection. A "UserID/Password" is handled in a similar fashion with out regard to how generated or whether it refers to a particular individual or a particular site. For a detailed description of this operation, the Examiner should consult Figs. 2 and 10-14, along with pages 14-16 and 33-39.

With regard to claims 2-5, 7-10, 12-15, and 17-20, the Examiner states:

> Claims 2-5, 7-10, 12-15, and 17-20 are also rejected as being non-enabled, inheriting the deficiencies of their parent independent claims, and furthermore because other claimed details, such as the "special field" of claims 3, 7, 13, and 17, and the mechanism for generation of the site specific security profile by the database management system (claims 3 and 6), are not disclosed in the specification. (Emphasis added)

For a detailed description of the "special field", to include its format, it is suggested that the Examiner consult Fig. 14 with special attention to Message #2. For a detailed description of "generation of the site specific security profile by the database management system", the Examiner should consult Figs. 11-14 and pages 33-36, of the specification, with particular attention to Fig. 13. The specification describes Figs. 13 and 14 at page 11, lines 1-4:

> **Fig. 13** is a diagram showing the creation of a site security profile; and
> **Fig. 14** is a listing of the messages utilized in creating the site security profile.

Because these drawings are quite "verbal" and are deemed essentially self-explanatory to those of ordinary skill in the art, the accompanying descriptions in the specification are somewhat brief.

Claims 1-20 have been rejected under 35 U.S.C. 112, second paragraph, as being indefinite. This rejection is respectfully traversed for the reasons provided above.

The Examiner has rejected all pending claims under 35 U.S.C. 103(a) as obvious in view of various combinations of at least three references. At paragraph 15, he curiously misquotes the Supreme Court's instructions to the lower courts in *Graham v. John Deer Co.* The Examiner does not even attempt to make any of these factual findings, because he cannot. The Examiner simply does not have the evidence presented to him as does a court in an *inter partes* proceeding.

For that reason, the Examiner is obligated to conduct his examination in this regard in accordance with MPEP 2143 which presents the requirements for the Examiner to make a *prima facie* case of obviousness. The three showings required are: 1)motivation to make the alleged combination; 2)reasonable likelihood of success of the alleged combination; and 3)all claim elements present in the alleged combination. The Examiner has made none of these showings. As a result, the rejection of claims 1-20 under 35 U.S.C. 103(a) is respectfully traversed for failure of the Examiner to present a *prima facie* case of obviousness.

Specifically, the Examiner has rejected claims 1-4, 6-8, 11-14, and 16-18 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison") in view of U.S. Patent 6,237,023, issued to Yoshimoto (hereinafter referred to as "Yoshimoto") further in view of the article, "Access Control in Federated Systems", by De Capitani di Vimercate et al (hereinafter referred to as "di Vimercati"). This ground of rejection is respectfully traversed.

In rejecting claim 1, the Examiner freely admits that Garrison does not employ a site-specific security profile. In fact, Garrison states at column 14, lines 5-7:

> Due to the security features described hereinabove, the database system 19a is effectively secured rom access by unauthorized users.

In other words, Garrison, which is a later disclosure than either Yoshimoto or di Vimercati, employs encryption of the password and has no need of a site-specific security profile. Nevertheless, the Examiner disregards the clear teaching of Garrison and states:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see Yoshimoto, col. 6, lines 15-21).

As a result, one reading Garrison would not be motivated to employ a site-specific security profile, because Garrison teaches that it is not necessary. The Examiner does not even mention the requirement of MPEP 2143 to show "reasonable likelihood of success".

Having admitted that neither Garrison nor Yoshimoto teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network, the Examiner has alleged the combination of yet another reference, di Vimercati. The Examiner clearly erroneously states:

> De Capitani di Vimercate et al, however, teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

The Examiner's statement is clearly erroneous, because none of the citations say anything of not transferring a user identifier.

Furthermore, the di Vimercati reference actually teaches away from the Examiner's conclusion. It states at paragraph 2.1:

A good user's authentication is a prerequisite for a correct access control. The identity of a user determines the groups to which the user belongs, the roles he can play (if applicable), and ultimately the privileges he is allowed to exercise. Even in mandatory systems, where clearances are used to access controls instead of identifiers, the user's identity is needed to determine the security level with which the user can connect to the system. In any case therefore, on a user's identity depends whether his requests to access the data will be allowed or denied. (Emphasis added)

Though di Vimercati is difficult to understand, it is apparent that transfer of the user identification is the principle element of the security process. This theme is repeated over and again. At paragraph 3.2, the reference states:

> To access a federation, a user must explicitly open a working session by connecting to the federation site. Connection requires identification of the user and corresponding authentication of his identity by the federation. (Emphasis added)

Thus, it is not readily understandable how the Examiner can make his clearly erroneous finding of fact.

Quite apart from di Vimercati saying nothing of transferring anything "via said publicly accessible digital data communication network", just like Garrison and Yoshimoto, di Vimercati considers that "the user's identity is needed to determine the security level". For the Examiner to argue differently is to deny the clear teachings of the references.

Having alleged the combination of three separate and mutually exclusive approaches, the Examiner states:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since (sic) they are all concerned with the same field of endeavor, that is, remotely accessing databases.

Having shown that all three references deem it necessary to transfer the user identifier over the network, the credibility of the Examiner's position is further eroded by his statement:

> It would have been furthermore obvious........whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since (sic) it is necessary to protect all information transferred over the global communication network.

The Examiner does not even address the other required showings. The rejection of claim 1, and all claims depending therefrom is respectfully traversed.

In rejecting claim 6, the Examiner states:

> c) a security profile generated by said database management system corresponding to said site whereby said database management system provides access to a particular portion of said database corresponding to said security profile (see col. 7, line 50 through col. 8, line 37).

This finding is clearly erroneous and completely inconsistent with the Examiner's own finding that:

> Garrison does not explicitly teach an apparatus wherein the security profile is site-specific.

Though claim 6 is limited by "a security profile generated by said database management system", the Examiner confusingly cites the Abstract and column 1, line 63, through column 2, line 6, of Yoshimoto which say nothing of "a security profile generated by said database management system". In fact the citations to Yoshimoto say nothing of a "security profile", thus rendering the Examiner's statement clearly erroneous:

> Yoshimoto, however, teaches an apparatus wherein the security profile is site-specific.

The Examiner concludes his rejection of claim 6 by clearly erroneously stating:

> De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

Though the reference teaches nothing of <u>not</u> transferring the user identifier, as explained above, it does state "the user's identity is <u>needed</u> to determine the security level". The rejection of claim 6 is respectfully traversed as based upon numerous clearly erroneous findings of fact.

In rejecting claim 11, the Examiner states:

> Garrison teaches.......signing on to said user terminal by said user utilizing said user identifier (see col. 2, lines 64 through col. 3, line 2, disclosing that the client transmits a password to the <u>client</u>....(emphasis added)

This statement is clearly erroneous and misquotes the citation. Garrison actually states:

> ....the client initially transmits a password to the server.... (emphasis added)

The Examiner proceeds by stating:

> ....meaning that the user has necessarily signed on to the client system utilizing a user identifier.

Apparently, the Examiner has made a finding of "inherency" without meeting his burden of proof under MPEP 2112. This finding is therefore not only clearly erroneous as a matter of fact, it is incorrect as a matter of law.

The rejection of claim 11 is respectfully traversed as based upon clearly erroneous findings of fact and incorrect application of controlling law.

Claim 16 is limited by:

> means.....for preventing....unless said site corresponds to a security profile.....

The Examiner clearly erroneously finds this limitation in Garrison citing column 6, line 60, through column 7, lines 32, and column 7, line 50 through column 8, line 37. The Examiner then contradicts his own finding stating that Garrison does not contain this limitation.

The Examiner then clearly erroneously states:

> Yoshimoto, however, teaches an apparatus wherein the security profile is site-specific (see Abstract, see also col. 1, line 63 through col. 2, line 6).

Yoshimoto says nothing of the claimed "security profile". To compound the error, the Examiner misquotes di Vimercati stating:

> ....see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access.

The cited portion of di Vimercati actually states:

> Connection requires identification of the user and corresponding authentication of his identity by the federation.

The rejection of claim 16, and all claims depending therefrom, is respectfully traversed as based upon clearly erroneous findings of fact.

In rejecting claim 2, the Examiner clearly erroneously states:

> Regarding claim 2, Garrison additionally teaches an improvement wherein said security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

The Examiner has admitted that Garrison does not teach an apparatus wherein the security profile is site-specific. Therefore, it is clearly erroneous to state that Garrison teaches "wherein said security profile is generated by said data management system. The rejection of claim 2 is respectfully traversed as based upon clearly erroneous findings of fact.

In rejecting claims 3, 8, 12-13, and 18, the Examiner clearly erroneously states:

> Regarding claims 3, 8, 12, 13 and 18, Garrison additionally teaches an improvement, method and apparatus further comprising a special field responsively coupled to a service requests whereby said database management system receives said special field and generates said security profile corresponding to said site and to said special field (see discussion of predefined password at col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37). (emphasis added)

Having admitted that Garrison does not have a "security profile corresponding to said site", it is baffling to see that the Examiner can find Garrison to contain these limitations.

In rejecting claims 5, 9, 10, 15, 19, and 20, the Examiner adds the King reference to the alleged combination of Garrison, Yoshimoto, di Vemercati stating:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER is extremely versatile and is considered one of the best fourth generation programs, and furthermore since it contains, in addition to a database management system, a word processor, office automation program including electronic mail, and color graphics routines (see King, first paragraph).

This statement is deemed clearly erroneous. The specification states at page 3, line 21, through page 4, line 6, states:

> However, with the MAPPER system, as well as with similar proprietary data base management systems, the user must interface with the data base using a terminal coupled directly to the proprietary system and must access and manipulate the data using the MAPPER command language of MAPPER. Ordinarily, that means that the user must either be co-located with the hardware which hosts the data base management system or must be coupled to that hardware through dedicated data links. Furthermore, the user usually needs to be schooled in

the command language of MAPPER (or other proprietary data base management system) to be capable of generating MAPPER Runs.

These specific characteristics of MAPPER are deemed so inconsistent with the goals of Garrison, Yoshomoto, and di Vimercati, one or ordinary skill in the art would not look to make the alleged combination.

The rejection of claims 5, 9, 10, 15, 19, and 20 is respectfully traversed.

Having thus responded to each objection and ground of rejection, Applicants respectfully request entry of this amendment and allowance of claims 1-20, being the only pending claims.

Respectfully submitted,

Paul S. Germscheid, et al

By their attorney,

Date December 8 , 2003

John L. Rooney
Reg. No. 28,898
Suite 401
Broadway Place East
3433 Broadway Street N.E.
Minneapolis, Minnesota
55413
(612) 331-1464